(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 September 2001 (20.09.2001)

PCT

(10) International Publication Number
WO 01/69838 A2

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/IB01/00346

(22) International Filing Date: 12 March 2001 (12.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/526,050 15 March 2000 (15.03.2000) US

(71) Applicant: NOKIA CORPORATION [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(71) Applicant *(for LC only)*: NOKIA, INC. [US/US]; 6000 Connection Drive, Irving, TX 75039 (US).

(72) Inventors: KUIKKA, Antti; Korvenkatu 36 as 2, FIN-33300 Tampere (FI). HONKANEN, Jukka-Pekka; Opiskelijankatu 18 A 16, FIN-33720 Tampere (FI).

(74) Agents: KELLY, Robert, H. et al.; Novakov Davis & Munck, P.C., 900 Three Galleria Tower, 13155 Noel Road, Dallas, TX 75240 (US).

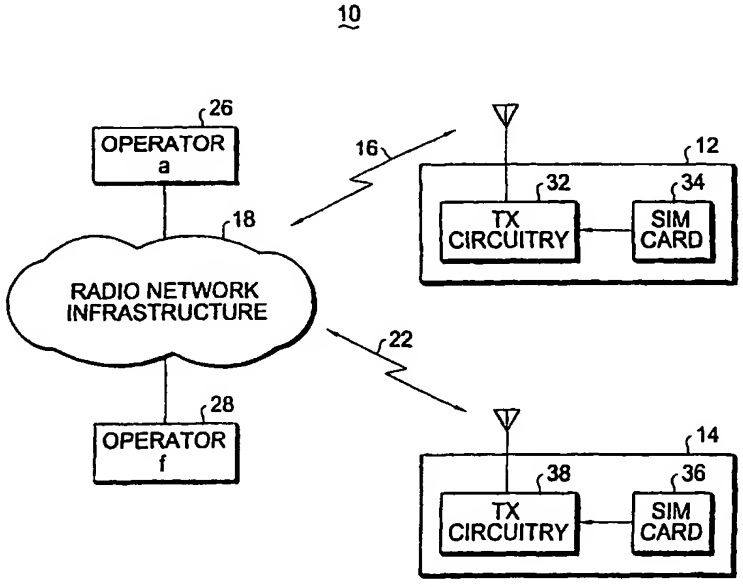
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: METHOD, AND ASSOCIATED APPARATUS, FOR GENERATING SECURITY KEYS IN A COMMUNICATION SYSTEM



(57) Abstract: A method (44), and an associated apparatus, is provided for exchanging security keys between mobile terminals (12, 14) operable in a GSM cellular, or other, communication system (10). When implemented in a GSM cellular communication system (10), SIM-card (34, 36) information is utilized in the generation of the keys which are exchanged between the mobile terminals (12, 14) and thereafter are utilized to secure data which is to be transmitted between the mobile terminals (12, 14) during a communication session.

WO 01/69838 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD, AND ASSOCIATED APPARATUS, FOR GENERATING SECURITY KEYS IN A COMMUNICATION SYSTEM

The present invention relates generally to the communication of data, such as IP (Internet Protocol)-formatted data, in a communication system, such as a GSM (Global System for Mobile communications) cellular communication system. More particularly, the present invention relates to a method, and associated apparatus, by which to perform security key generation pursuant to the IPsec (Security Architecture for Internet Protocol) to facilitate secured communications of packet data between two communication stations, such as two mobile terminals operable in the GSM communication system.

When implemented in a GSM communication system, advantageous use is made of the security algorithms and procedures stored at a SIM (Subscriber Identity Module)-card positioned at the mobile terminals.

BACKGROUND OF THE INVENTION

The use of wireless communication systems has achieved wide popularity in recent years as a result of advancements in communication technologies. Multi-user, wireless communication systems of improved capabilities are regularly utilized by large numbers of consumers to communicate both voice and nonvoice information.

In a wireless communication system, a communication channel formed between a sending station and a receiving station is a radio channel defined upon a portion of the electromagnetic spectrum. Because a radio channel forms a communication link between the sending and receiving stations, a wireline

connection is not required to be formed between the sending and receiving stations to permit the communication of data between the stations. Communication by way of a wireless communication system is thereby permitted at, and between, locations at which the formation of a wireline connection would not be practical. Also, because a communication channel is formed of a radio channel, a radio communication system can be more economically installed as the infrastructure costs associated with a wireline communication system are significantly reduced.

A cellular communication system is exemplary of a wireless, multi-user radio communication system which has achieved wide levels of usage and which has been made possible due to advancements in communication technologies. A cellular communication system is typically formed of a plurality of fixed-site base stations installed throughout a geographical area which are coupled to a PSTN (Public-Switched, Telephonic Network). Portable transceivers, typically referred to as mobile stations, or mobile terminals, communicate with the base stations by way of radio links.

A cellular communication system efficiently utilizes the portion of the electromagnetic spectrum allocated thereto. Because of the spaced-apart positioning of the base stations, only relatively low-power signals are required to effectuate communications between a base station and a mobile station. As a result, the same frequencies can be reused at different locations throughout the geographical area. Thereby, communications can be effectuated between more than one set of sending and

receiving stations concurrently at separate locations throughout the area encompassed by the cellular communication system.

Digital communication techniques are also utilized in many cellular, as well other types of, communication systems. Utilization of digital communication techniques, for instance, permits the increase of communication capacity and, also as a result thereof, have permitted the introduction of new types of communication services. Digital communication techniques have facilitated improvements in the maintenance of security in communications effectuated during operation of such communication systems. Various measures have been taken with respect to security issues, of significance particularly in radio communication systems. For instance, procedures are set forth to ensure that access is granted to mobile terminals to communicate by way of the communication system only subsequent to their authentication as being authorized to communicate therethrough. In GSM communication systems, an authentication procedure is set forth in which ciphering keys are utilized in a public/private ciphering scheme to perform the authentication procedures. A storage element, referred to as a SIM (Subscriber Identity Module) card contains the necessary information to perform the authentication procedures. Also, data encryption, prior to its communication upon a communication channel, and corresponding de-encryption once received at another communication station is provided for in GSM communication systems. Information stored at the SIM-card is also utilized for encrypting data.

In digital communication systems, increasingly, communication is effectuated through the communication of packets of data, such as packets of data formatted pursuant to a TCP/IP (Transport Control Protocol/Internet Protocol) protocol. While security procedures for IP-formatted data have been set forth, such existing procedures do not well make use of the information stored on the SIM cards of mobile terminals operable in a GSM communication system. Conventionally, public key encryption, such as PGP (Pretty Good Privacy) encryption, and the use of a certification authority (CA) have more generally been utilized. Such existing procedures, while utilizing a relatively simple key exchange, suffers from the drawback that delivery of a public key to the certification authority is difficult. For instance, the extent to which the certification authority is able to trust a public key delivered thereto belongs to the participant.

If a manner could be provided by which to utilize the information already stored at a SIM card in an IPsec key exchange, improved security procedures would be possible.

It is in light of this background information related to the security architecture for Internet protocol that the significant improvements of the present invention have evolved.

SUMMARY OF THE INVENTION

The present invention, accordingly, advantageously provides a method, and associated apparatus, by which to perform security key generation in a communication system, such as a GSM (Global

System for Mobile communications), or other, cellular communication system.

Through operation of an embodiment of the present invention, a key exchange protocol is utilized which removes a so-called man in the middle attack to the protocol. All messages are operated through an entity. In an implementation in which IP data is to be communicated between two mobile terminals operable in a communication system, messages are routed through an operator, or operators, of the GSM authentication, or other, communication system.

Thereby, secured communication of packet between two mobile terminals operable with the GSM, or other, communication system is facilitated. When implemented in a communication system, advantageous use is made of the security algorithms and other information stored at a SIM (Subscriber Identity Module)-card positioned at the mobile terminal to generate the security keys. Analogously, the corresponding information stored at the network infrastructure of the GSM communication system is also advantageously used to facilitate such generation of the security keys.

In one implementation, a manner is provided by which to exchange security keys between two mobile terminals operable in a GSM cellular, or other, communication system in which both of the mobile terminals communicate with the same operator. In such an implementation, the single operator personalizes the information stored at the mobile terminal and also stores the information at the operator. Thereby, secured key exchanges are effectuable between the first mobile terminal and the operator and between the operator and the second mobile terminal. Subsequent to such exchange of keys, i.e., in which the messages

communicated between the mobile terminals and the operator are signed and/or encrypted by ciphering keys, secured data communication is possible between the two mobile terminals. Secured data transmission is effectuated by encrypting the data to be communicated therebetween by a secret key generated pursuant to the key exchange effectuated by way of the operator.

In the implementation in which the communication system is formed of a GSM cellular communication system, the mobile terminals include SIM-cards which contain information personalized by the operator of the GSM system. Authentication algorithms as well as a ciphering key and the identity of the mobile terminal are stored at the SIM-card. Such information is utilized to generate a pseudo random number, a first ciphering key, and the identity of the second mobile terminal to which IP-formatted data is to be communicated. Such information is forwarded to the operator which performs analogous operations and also determines the identity of the second mobile terminal to which the IP-formatted data is ultimately to be communicated in a communication session between the first and second mobile terminals. The operator generates a second ciphering key together with a second pseudo random number and forwards such information together with the identity of the first mobile terminal to the second mobile terminal. The second mobile terminal detects the transmitted information and generates a new secret key to be used for data transmission between the first and second mobile terminals. The second mobile terminal also determines the identity of the first mobile terminal responsive to the message sent thereto by the

operator. The key is utilized thereafter to sign, or encrypt, messages communicated between the first and second mobile terminals.

In another implementation, information stored at a first of the mobile terminals is personalized by a first operator, and the information stored at a second of the mobile terminals is personalized by a second operator. The separate operators operate separate portions of the communication system. In such an implementation, a first secured key exchange is performed between the first mobile terminal and the first operator. Then, pursuant to a key generation query, a secured key exchange is performed between the first operator and the second mobile terminal. Thereafter, ciphering keys are generated to facilitate the transmission of secured data between the first and second mobile terminals. In another such implementation, subsequent to the generation of the first ciphering key pursuant to the secured key exchange between the first mobile terminal and the first operator, a secured key exchange is performed between the second mobile terminal and the second operator. And, a third ciphering key is generated and utilized to secure data to be transmitted between the first and second mobile terminals.

In these and other aspects, therefore, a method, and an associated assembly, is provided for communicating in a communication system having at least a first communication system portion operated by a first operator. The first operator is coupled to the network infrastructure of the communication system. The communication system has a first communication station operable at least to communicate packet data and a second communication station also

operable at least to communicate packet data. Security keys are generated for use to secure the packet data communicated between the first communication station and the second communication station. A first ciphering key is generated at the first communication station. The first ciphering key is then forwarded to the network infrastructure together with indicia identifying the second communication station. A message is thereafter routed to the second communication station. And, secret keying material to be exchanged between the first communication station and the second communication station is generated.

A more complete appreciation of the present invention and the scope thereof can be obtained from the accompanying drawings which are briefly summarized below, the following detailed description of the presently-preferred embodiments of the invention, and the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a functional block diagram of a radio communication system in which an embodiment of the present invention is operable.

Figures 2A-2B illustrate a message sequence diagram listing the sequence of operation of an embodiment of the present invention to exchange security keys to facilitate the transmission of secured data between the first and second mobile terminal shown in Figure 1.

Figures 3A-3B illustrate another message sequence diagram, also illustrating the sequencing of messages generated during operation of another embodiment of the present invention.

Figures 4A-4B also illustrates a message sequence diagram, also illustrating the sequencing of messaging generated during operation of another embodiment of the present invention.

Figure 5 illustrates a message sequence diagram illustrating in greater detail portions of the sequences shown in Figures 3A-B and 4A-B.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring first to Figure 1, a communication system, shown generally at 10, is operable to provide for radio communications with mobile terminals, of which a first mobile terminal 12 and a second mobile terminal 14 are exemplary. In the exemplary implementation, the communication system 10 forms a GSM (Global System for Mobile communications) cellular communication system operable pursuant to an appropriate standard. While the present invention shall be described with respect to an exemplary implementation in a GSM communication system, operation of an embodiment of the present invention is analogously operable and such operation can be analogously described.

The mobile terminal 12 is operable to transceive communication signals by way of radio link 16 with the network infrastructure 18 of the communication system. Similarly, the mobile terminal 14 is operable to transceive communication signals by way of the radio link 22 with the network infrastructure 18. The mobile terminal 12 is, for example, able to communicate with the mobile terminal 12 by way of a communication path which includes the radio links 16 and 22 and portions of the network infrastructure 18. Each of the mobile terminals 12 and 14 is also capable

of communicating with other communication stations (not shown), such as a communication station coupled to a PSTN (Public-Switched, Telephonic Network).

A first operator, operator a, 26, and a second operator, operator f, 28, are also shown to form a portion of the communication system. The operators a and f are coupled to the radio network infrastructure 18 to form a portion thereof. In conventional manner, the operators control operation of portions of the communication system.

In the exemplary implementation in which the communication system forms a GSM cellular communication system, the mobile terminal 12 includes, in addition to transceiver circuitry 32, a SIM (Subscriber Identity Module)-card 34. The SIM-card is conventional of a GSM SIM-card, typically removable from the mobile terminal. The SIM-card includes, for instance, a unique identifier, IDb which identifies the SIM-card and, hence, the mobile terminal 12 to which the card is connected. A subscriber authentication key, Ki, is also stored at the SIM-card, as are authentication and A3 and A8 algorithms. The A8 algorithm, for instance, is a ciphering key generation algorithm. The information stored at the SIM-card 34 is utilized during operation of an embodiment of the present invention.

The second mobile terminal 14 in such an implementation, also includes a SIM-card 36 in addition to transceiver circuitry 38. The information stored at the SIM-card 36 is similar to that stored at the SIM-card 34, individualized for the specifics of the mobile terminal 14. For instance, the identity, IDd, of the mobile terminal 14 is stored at the SIM-card 36 rather than the IDb stored at the SIM-card 34.

Operation of an embodiment of the present invention provides a manner by which to exchange security keys between the mobile terminals pursuant to IPsec, the security architecture for Internet protocol, through the use of the information stored at the SIM-cards 34 and 36.

Figures 2A-2B illustrate a message sequence diagram, shown generally at 44, illustrating operation of an embodiment of the present invention to exchange security keys between mobile terminals 12 and 14, thereby to permit secured data transmission therebetween. The message sequence diagram 44 shown in Figure 3 is representative of operation of the communication system in which both mobile terminals 12 and 14 are operated by the operator a, 26. And, here, the mobile terminal 12 is represented by the SIM-card b, 34, in which the mobile terminal 12 is utilized by a user c. And, the mobile terminal 14 is represented by the SIM-card d, 36, and the mobile terminal is operated by a user e.

Communications are initiated by the user of the mobile terminal 12, as indicated by the block 46. The block 48 indicates the items known at the mobile terminal 12 at the initiation of the communication session. In addition to the information mentioned previously to be stored at the SIM-card 34, the IP address (IPa) of the operator a, 26, the IP address of the user c (IPc), and the IP address of the user of the mobile terminal 14 (IPe) are known by the mobile terminal 12. The block 48 also indicates that a value of a pseudo random number, RANDfill is generated.

Then, and as indicated by the block 50, SK and TID generation is performed to form SKca values at both the terminal 12 and at the operator a 26.

Additional details relating to SK and TID generation shall be described with respect to Figure 5 below.

A message 55, KEYGEN(TIDb,E{RANDfill,IPc,IPe}SKca, S{RANDfill,IPc,IPe}SKca} is generated by the mobile terminal 12, including the information it generated, or otherwise known at the mobile terminal 12 and communicated to the operator a, 26.

Thereafter, and as indicated by the block 58, the operator a decrypts the encrypted values of IPc and IPe provided thereto in the message 55.

Block 62 indicates items known at the operator a. Namely, IDd is the identity of the SIMd 36 of the mobile terminal 14. Such value is known by both the operator a and also at the SIM-card d, 36. The subscriber authentication key Ki stored in the SIM-card d 36 is also known by the operator a, as are the algorithms A3 and A8 stored at the SIM-card d 36. Additionally, the IP addresses of the operator a (IPa), of the user c (IPc), and of the user e (IPe) are also known by the operator a. The value of IPe matches that of IDd.

Then, and as indicated by the block 63, the operator a generates a pseudo random number RANDea of 128 bits. The number is generated at an AUC (Authentication Center) associated with the operator, as are also "triplets" including values of RAND, SRES, and Kc for the requested SIM card, here IDd.

At the block 64, the operator a 26 generates new secret keying material, SKea to be used between the user e of the mobile terminal 12 and the operator a. The operator a concatenates Kc:s to TKea in which TKea is executed using a one-way algorithm Aow by which to generate SKea. The resultant output, SKea, is used as

secret keying material between the user e and the operator a. Block 66 indicates that operator a knows that the user e of the mobile terminal 14 uses an operator a-personalized SIM-card.

As indicated by the message 68 transmitted by the operator a 26 to the mobile terminal 14, information formed at, or otherwise known by, the operator a, is communicated to the mobile terminal 14. Here, the message is indicated by

KEYGEN(RANDea,S[RANDea]SKea,E[IPc,IPe]SKea).

Block 72 indicates that selection is made by the user e of the mobile terminal to accept a secured data link with what, to the user e, is a currently-unknown user, i.e., user c of the mobile terminal 12. Block 74 indicates that the user e of the mobile terminal 14 generates new secret keying material, SKea, to be used between the user e and operator a. The user e splits the RANDea to 128-bit blocks. Each block is executed through a SIM A8 algorithm. The output is a 64-bit length Kc from each block. Again, alternately, the algorithm A3 could instead be utilized to form a 32-bit length SRES value. The results are concatenated to TKea, and TKea is executed by way of the one-way algorithm Aow. The output SKea is used as secret keying material between the user e and the operator a. Block 76 indicates that the user e of the mobile terminal 14 decrypts the message indicated by the segment 68 to obtain a value of IPc, i.e., the user c of the mobile terminal 12.

As the operations indicated by the block 72, 74, and 76 are being performed, at the mobile terminal 12, and as indicated by the block 78, the user c of the mobile terminal 12 selects a value of a Diffie-Hellman group to be used in a Diffie-Hellman exchange. Also,

a value of y and g^y are calculated. Then, and as indicated by the message 82, such information is communicated from the mobile terminal 12 to the operator a 26. Such message is indicated by KEYEX(E{GRP,g^y}SKea).

When the message 82 is detected by the operator a, as indicated by the block 84, the operator decrypts the message to obtain values of the variable of the Diffie-Hellman group and a value of g^y.

Then, and as indicated by the message 86, such values, together with a value SKea are communicated from the operator a 26 to the mobile terminal 14. The message is indicated KEYEX(E{GRP,g^y}SKca). Once received at the mobile terminal 14, and as indicated by the block 88, the user e decrypts the message 86 to obtain the values of GRP and g^y. Then, and as indicated by the block 92, the user e uses the values of GRP to generate x and to calculate the value g^x.

Thereafter, and as indicated the message 94, such information is communicated from the mobile terminal 14 to the operator a 26. The message is indicated by KEYEX(E{GRP,g^x}SKea). Received at the operator a, and as indicated by the block 96, the operator decrypts the message to obtain values of GRP and g^x. Thereafter, and as indicated by the message 98, such information is forwarded from the operator a to the mobile terminal 12.

Once detected thereat, and indicated by the block 102, the user c of the mobile terminal 12 decrypts the message to obtain values of GRP and g^x. Then, and as indicated by the block 104, the user c generates secret keying material from SKce which is equal to (g^x)^y which is equal to g^(xy). Then, as indicated by the block 106, the user c encrypts the data to be

communicated to the mobile terminal with the key SKce. Block 108 indicates that the user e of the mobile terminal 14 also generates secret keying material SKce in the same manner.

The encrypted data, encrypted with SKce is communicated from the mobile terminal 12 to the mobile terminal 14, as indicated by the message 112. The message 112 is represented by E{(data)}SKce. When detected at the mobile terminal 14, and as indicated by the block 114, the user e decrypts the encrypted data provided thereto with the key SKce. A response to be communicated by the mobile terminal 14 to the mobile terminal 12 is encrypted, indicated by the block 116, with the key SKce. And, the response is communicated in the form of a message 118 to the mobile terminal 12. The message is indicated by E{(response)}SKce.

Figures 3A-3B illustrate a message sequence diagram, shown generally at 112, illustrating signaling generated during operation of another embodiment of the present invention. Here, again, keys are exchanged between the first and second mobile terminal 12 and 14 to be used to secure data to be transmitted between the mobile terminals. In this implementation, operator a 26 and operator f 28 are associated with the respective mobile terminals 12 and 14.

First, and as indicated by the block 124, selection is made at the mobile terminal 12 by the user c thereof to initialize a secured data link with the user e of the mobile terminal 14. Block 126 indicates that the items known at the mobile terminal 12 include the identification of the SIMb, IDb. Also, the subscriber authentication key Ki and the

algorithms A3 and A8, as well as the IP addresses of the operator a, the user c, and the user e IPa, IPc, and IPe are all known. The block 126 also indicates that a value of a pseudo random number RANDfill is generated.

Then, and as indicated by the block 130, SK and TID generation is performed to form SKca and TIDb values at both the terminal 12 and at the operator a. Additional details relating to SK and TID generation shall be described with respect to Figure 5 below.

The information generated at, or otherwise known to, the mobile terminal 12 is communicated, indicated by the message 134, by the mobile terminal to the operator a. Here, the message is indicated by KEYGEN(TIDb,E{RANDfill,IPa,IPc,IPe}SKca,{RANDfill,IPa, IPc,IPe} SKca).

Then, and as indicated by the block 138, the operator decrypts the encrypted values of IPc and IPe contained in the message 134. Then, and as indicated by the block 142, the operator generates a pseudo random number RANDaf which is used to separate different parallel key generation, and is an ID to a session where keys are used. Then, and as indicated by the message 144 communicated by the operator a to the mobile terminal 14, the value of RANDaf is transmitted. The message is represented by KEYGEN(RANDaf).

As indicated by the block 146, selection is made by the user e of the mobile terminal 14 to accept a secure data link with what, with respect to the user e, is a currently-unknown user. Block 148 indicates that the items known at the mobile terminal 14 include the identification of the SIMd card, IDd. Such value is known both by the operator f 28 and the mobile

terminal 14. The subscriber authentication key Ki, as well as the algorithms A3 and A8 are also known at the mobile terminal as are also the IP addresses of the operator a, the operator f, and the user e, i.e., IPa, IPf, and IPe. A pseudo random number RANDef is also shown to be generated at the block 148. The RANDfill value is of a length of 128 bits. Then, and as indicated by the block 150, SKxy generation is performed, here to form values of SKef and TIDd. Again, additional details regarding such generation shall be described with respect to Figure 5.

Then, and as indicated by the message 156, such information generated at, or known by, the mobile terminal 14 is communicated therefrom to the operator f. The message is represented by KEYGEN (RANDfill,RANDaf, IPa,IPe).

Then, and as indicated by the block 158, the operator detects the message 156.

Thereafter, and as indicated by the block 164, SKef is sent from the operator f 28 to the operator a 26. A message 166 is shown to be communicated by the operator f to the operator a. The message is represented by KEYGEN(RANDaf,SKef,IPa,IPe). Block 168 indicates that the RANDaf forms the ID to the communication session in which the key SKef is used. And, the block 172 indicates that the user c of the mobile terminal 12 selects a Diffie-Hellman group variable GRP, generates y, and calculate g^y . Then, a message 174 is communicated by the mobile terminal 12 to the operator a 26. The message is represented by KEYEX(E{GRP,g^y,IPc,IPe}SKca).

Thereafter, and as indicated by the block 176, upon detection of the message, the operator a decrypts the message to obtain values of IPc, IPe, GRP, and

g^y. And, a message 178 is communicated from the operator a to the second mobile terminal 14. The message is represented by KEYEX(E{RANDaf,GRP,g^y,IPc,IPe}SKef).

When the message 178 is detected by the mobile terminal 14, and as indicated by the block 182, the user e of the mobile terminal decrypts the message received thereat to obtain values of RANDaf, IPc, IPe, GRP, and g^y. Resultant therefrom, and as indicated by the block 184, the user e of the mobile terminal becomes aware that user c is the other participant to the communication session. Then, and as indicated by the block 186, the user e generates x and calculates g^x.

Thereafter, a message 188 is communicated from the mobile terminal 14 to the operator a 26. The message 188 is represented by KEYEX(E {RANDaf,GRP,g^x,IPc,IPe}SKef). When detected at the operator a, and as indicated by the block 192, the operator a decrypts the message to obtain values of RANDaf, IPc, IPe, GRP, and g^x. A message 194 is then communicated from the operator a to the first mobile terminal 12. The message is represented by KEYEX(E{RANDaf,GRP,g^x,IPc,IPe}SKca).

When the message 194 is detected at the first mobile terminal, and as indicated by the block 196, the user c of the mobile terminal decrypts the message to obtain values of RANDaf, IPc, IPe, GRP, AND g^x. Thereafter, and as indicated by the blocks 198 and 202, respectively, the user c generates secret keying material, SKce, by (g^x)^y = g^(xy) and encrypts data with the key SKce. And, as indicated by the block 204, the user e of the mobile terminal 14 also

generates secret keying material SKce by (g^y)^x = g^(xy).

Thereafter, an encrypted data message 206 is communicated from the mobile terminal 12 to the mobile terminal 14. The message is represented by E{(data)}SKce. When detected at the mobile terminal 14, and as indicated by the block 208, the user e of the mobile terminal 14 decrypts the encrypted data received thereat with the key SKce. A response by the mobile terminal 14 is generated, here represented by the block 212, and encrypted with the key SKce. A message 214 is returned by the mobile terminal 14 to the mobile terminal 12. The message is represented by E{(response)}SKce. Then, and as indicated by the block 216, the user c of the mobile terminal 12 decrypts the encrypted response received thereat with the key SKce. Thereby, secured transmission of data between the mobile terminals 12 and 14 is effectuated.

Figures 4A-4B illustrate a sequence diagram, shown generally at 222, also representative of operation of an embodiment of the present invention. The sequence diagram 222, analogous to the message sequence diagram 122 shown in Figure 3, represents operation of an embodiment of the present invention in which operator a 26 is associated with the first mobile terminal 12 and the operator f 28 is associated with the second mobile terminal 14. The operation is performed at various elements noted in the sequence diagram, and messages communicated between such elements correspond with like-numbered operations and messages shown in, and described with respect to, Figure 3. Namely, operations 124-130 performed at the mobile terminal 12, the message 134 communicated from the mobile terminal 12 to the operator a 26,

operations 138-142 performed at the operator a, the message 144 communicated by the operator a to the second mobile terminal 14, operations 146-150 performed at the mobile terminal 14, the message 156 communicated by the mobile terminal 14 to the operator f 28, and the operations 158 and 164 performed at the operator f correspond with such operations and messages described with respect to the sequence diagram 122 shown in Figure 3. Such operation shall not again be described. In the implementation represented by the sequence diagram 222, a message 228 is communicated by the first mobile terminal 12 to the operator a. The message is represented by KEYEX(E{GRP,g^y,IPc,IPe}SKca).

When the message 228 is detected at the operator a, and as indicated by the block 232, the operator a decrypts the received message to obtain values of IPc, IPe, GRP, and g^y. The RANDaf becomes the ID to the communication session in which the key SKef is utilized. Then, a message 234 is communicated by the operator a to the operator f 28. The message 234 is represented by KEYEX(RANDaf,GRP,g^y,IPc,IPe). Then, a message 236 is communicated by the operator f to the second mobile terminal 14. The message 236 is represented by KEYEX(E{GRP,g^y,IPc,IPe}SKef).

When received at the second mobile terminal, and as indicated by the block 238, the user e decrypts the message to obtain values of IPc, IPe, GRP, and g^y. Then, and as indicated by the block 242, as a result, the user e obtains knowledge that the user c is the other participant of the communication session. Then, and as indicated by the block 244, the user e of the mobile terminal 14 generates x and calculates g^x. Then, a message 246 is communicated by the second

mobile terminal operator f. The message is represented by KEYEX(E{GRP,g^x,IPc,IPe}SKef).

When the message 246 is detected at the operator f, and as indicated by the block 248, the operator decrypts the message to obtain values of IPc, IPe, GRP, and g^x. Then, a message 252 is communicated by the operator f to the operator a. The message is upon any secured link and is represented by KEYEX(RANDaf,GRP,g^x,IPc,IPe).

Thereafter, a message 254 is communicated by the operator a to the first mobile terminal 12. The message is represented by KEYEX (E{GRP,g^x,IPc,IPe}SKca).

When detected at the mobile terminal 12, the user c thereof decrypts the received message to obtain values of IPc, IPe, GRP, and g^x. Then, indicated by the blocks 258 and 262, the user c generates secret keying material, SKce, by (g^x)^y = g^(xy), and the data to be communicated by the mobile terminal 12 is encrypted with the key SKce. And, as indicated by the block 264, the user e of the second mobile terminal 14 generates secret keying material, SKce, by (g^y)^x = g^(xy).

Thereafter, a message 266 is communicated by the mobile terminal 12 to the mobile terminal 14. The message 266 is encrypted data and is represented by E{(data)}SKce. When detected at the second mobile terminal 14, the user e thereof decrypts the encrypted data with the key SKce, indicated by the block 268. A response message generated at the second mobile terminal is encrypted, as indicated by the block 272, with the key SKce. The response message 274 is communicated by the mobile terminal 14 to the mobile terminal 12. The message is represented by

E{(response)}SKce. When detected at the first mobile terminal 12, and as indicated by the block 276, the user c decrypts the encrypted response with the key SKce. Thereby, secured data communications are effectuated between the first and second mobile stations 12 and 14.

Figure 5 illustrates a message sequence diagram, shown generally at 302, which illustrates in greater detail the manner by which values of SK and TID are generated during operation of an embodiment of the present invention. The sequence 302 corresponds to the sequence steps 50 and 130 shown in Figures 2-4 and, by analogy, also step 150 shown in Figures 3-4.

As indicated by step 304, the user c of the mobile station 12 elects to initiate a secure data link with the user e of the mobile station 14.

Block 306 indicates that values of IDb, Ki, the IP addresses of the operator a, and users c and e, IPa, Ipc, and IPe, respectively, are known, as are the algorithms A3 and A8. And, block 306 also indicates that a temporary value of TIDb is generated at the mobile station 12.

Block 308 indicates that, at the operator a 26, values of IDd and Ki in the SIM d as well as values of the algorithms A3 and A8 are known.

Then, as indicated by the segment 312, a message KEYREQ(IDb,TIDb) is sent by the mobile station 12 to the operator a.

Block 314 indicates that, once the message is detected at the operator a, the value of TIDb is saved and a value of RANDca is calculated, here at an AUC (Authentication Center), along with, e.g., values of SRES and Kc. Then, as indicated by the block 316, a new key, SKca, to be used between the user c of the

mobile station 12 and the operator 26 is generated. The key is concatenated to TKca, which is executed by way of a one-way algorithm, to generate an output value of SKca. The output value of SKca is used as secret keying material.

Then, and as indicated by the segment 318, a message, KEYRAND (RANDca,TIDb,S{RANDca,TIDb}SKca), is sent by the operator a 26 to the mobile station 12.

When the message is detected at the mobile station, the detected value of TIDb is compared with the value formed thereat, as indicated by the block 322. The values should match. Finally, and as indicated by the block 324, the user c generates a value of SKca, and splits the RANDca value into 128 bit blocks in which each block is executed by an A8, or A3, algorithm. The results are concatenated to TKca which is executed by way of the one-way algorithm. Thereafter, the output value of SKca, formed therefrom, is used as secret keying material.

The preferred descriptions are of preferred examples for implementing the invention, and the scope of the invention should not necessarily be limited by this description. The scope of the present invention is defined by the following claims:

We claim:

1. In a method for communicating in a communication system having at least a first communication system portion operated by a first operator coupled to network infrastructure of the communication system, and the communication system having a first communication station operable at least to communicate packet data and a second communication station, also operable at least to communicate packet data, an improvement of a method for generating security keys for use to secure the packet data communicated between the first communication station and the second communication station, said method comprising:

generating a first ciphering key at the first communication station;

forwarding the first ciphering key to the network infrastructure together with indicia identifying the second communication station;

routing a message to the second communication station; and

generating secret keying material to be exchanged between the first communication station and the second communication station.

2. The method of claim 1 wherein the first communication station comprises a first mobile terminal operable in a cellular communication system, the first mobile terminal having a storage element for storing first-communication-system related information thereat, the first-communication-system related information used during said operation of generating the first ciphering key to generate the first ciphering key.

3. The method of claim 2 wherein the communication system comprises a GSM (Global System for Mobile communications) cellular communication system, wherein the first mobile terminal comprises a GSM-compatible mobile terminal the storage element thereof forming a SIM (Subscriber Identity Module) and wherein the first ciphering key generated during said operation of generating the first ciphering key is generated utilizing SIM-information stored at the SIM.

4. The method of claim 3 wherein the first ciphering key forwarded to the network infrastructure during said operation of forwarding the first ciphering key is forwarded to the first operator.

5. The method of claim 4 further comprising the operation, prior to said operation of routing, of generating a second ciphering key at the first operator.

6. The method of claim 5 wherein said operation of routing the message to the second communication station comprises routing the second ciphering key generated at the first operator to the second communication station together with indicia identifying the first communication station.

7. The method of claim 6 wherein the first operator operates at least a portion of the GSM cellular communication system of which the communication system is formed and the second ciphering key generated by the first operator is generated utilizing SIM-type information.

8. The method of claim 7 wherein the second communication station to which the second ciphering

key is forwarded also comprises a mobile terminal operable in the GSM cellular communication system.

9. The method of claim 7 wherein the secret keying material generated during said operation of generating the secret keying material is utilized to transmit secured data between the first mobile terminal and the second mobile terminal.

10. The method of claim 4 wherein the message routed during said operation of routing comprises a nonencrypted message utilizing SIM-type information.

11. The method of claim 10 comprising the additional operation, subsequent to said operation of routing, of generating a second ciphering key at the second mobile terminal.

12. The method of claim 11 wherein the communication system further has a second communication system portion operated by a second operator coupled to the network infrastructure of the communication system, said method further comprising the additional operation of forwarding the second ciphering key to the second operator.

13. The method of claim 12 comprising the additional operation of forwarding the seconding ciphering key to the first operator.

14. The method of claim 13 further comprising the additional operation of forwarding a message from the first operator to the second mobile terminal, the message including indicia identifying the first mobile terminal.

15. The method of claim 14 further comprising the additional operation of generating a third

ciphering key, the third ciphering key utilized during said operation of generating the secret material to generate the secret keying material.

16. In a method for communicating in a communication system having at least a first communication system portion and by a first operator coupled to network infrastructure of the communication system, and the communication system having a first communication station operable at least to communicate packet data and a second communication station, also operable at least to communicate packet data, an improvement of a method generating security keys for use to secure the packet data communicated between the first communication station and the second communication station, said method comprising:

generating a first ciphering key at the first communication station;

forwarding the first ciphering key to the first network infrastructure together with indicia identifying the second communication station;

generating a second ciphering key at the network infrastructure;

forwarding the second ciphering key to the second communication station together with indicia identifying the first communication station; and

utilizing the second ciphering key to generate secret keying material to be exchanged between the first communication station and the second communication station.

17. In a communication system having at least a first communication system portion operated by a first operator coupled to network infrastructure of the communication system, and the communication system

having a first communication station operable at least to communicate packet data and a second communication station, also operable at least to communicate packet data, an improvement of an assembly for generating security keys for use to secure the packet data communicated between the first communication station and the second communication station, said assembly comprising:

a first ciphering key generator located at the first communication station, said first ciphering key generator for generating a first ciphering key at the first communication station;

transmitter circuitry coupled to said first ciphering key generator, said transmitter circuitry for forwarding the first ciphering key to the network infrastructure together with indicia identifying the second communication station;

a router positioned at the network infrastructure, said router routing a message to the second communication station; and

a secret keying material generator located at both the first communication station and the second communication station, said secret material generator for generating secret keying material to be exchanged between the first communication station and the second communication station.

18. The assembly of claim 17 wherein the communication system comprises a GSM (Global System for Mobile communications) cellular communication system and wherein the first ciphering key generated by said first ciphering key generator utilizes SIM-type information.

19. The assembly of claim 18 wherein said router is located at the first operator.

20. The assembly of claim 19 further comprising a second ciphering key generator located at the first operator, said second ciphering key generator for generating a second ciphering key.

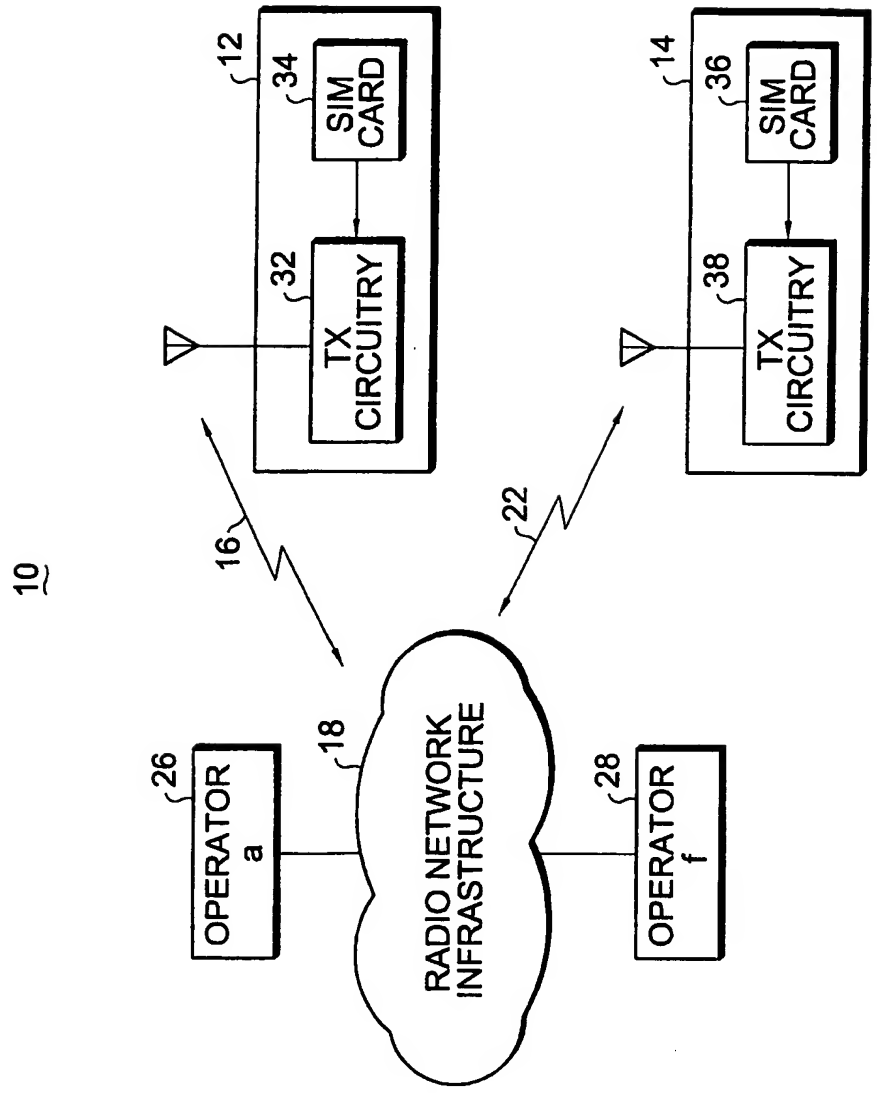

10
12
34
SIM CARD
32
TX CIRCUITRY
14
36
SIM CARD
38
TX CIRCUITRY
16
22
18
RADIO NETWORK INFRASTRUCTURE
26
OPERATOR a
28
OPERATOR f

FIG. 1

FIG. 2A
FIG. 2B
FIG. 2C

FIG. 2

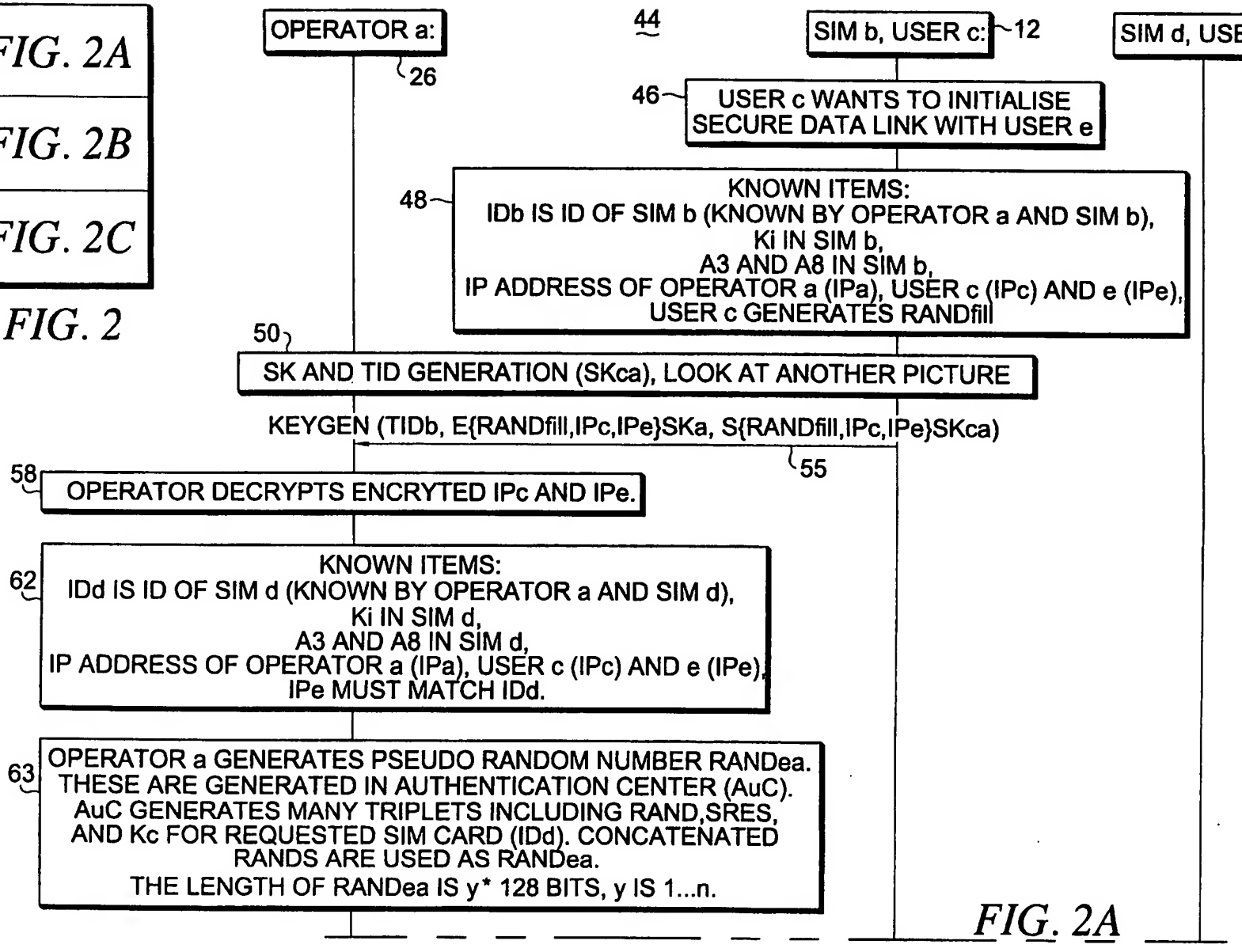


FIG. 2A

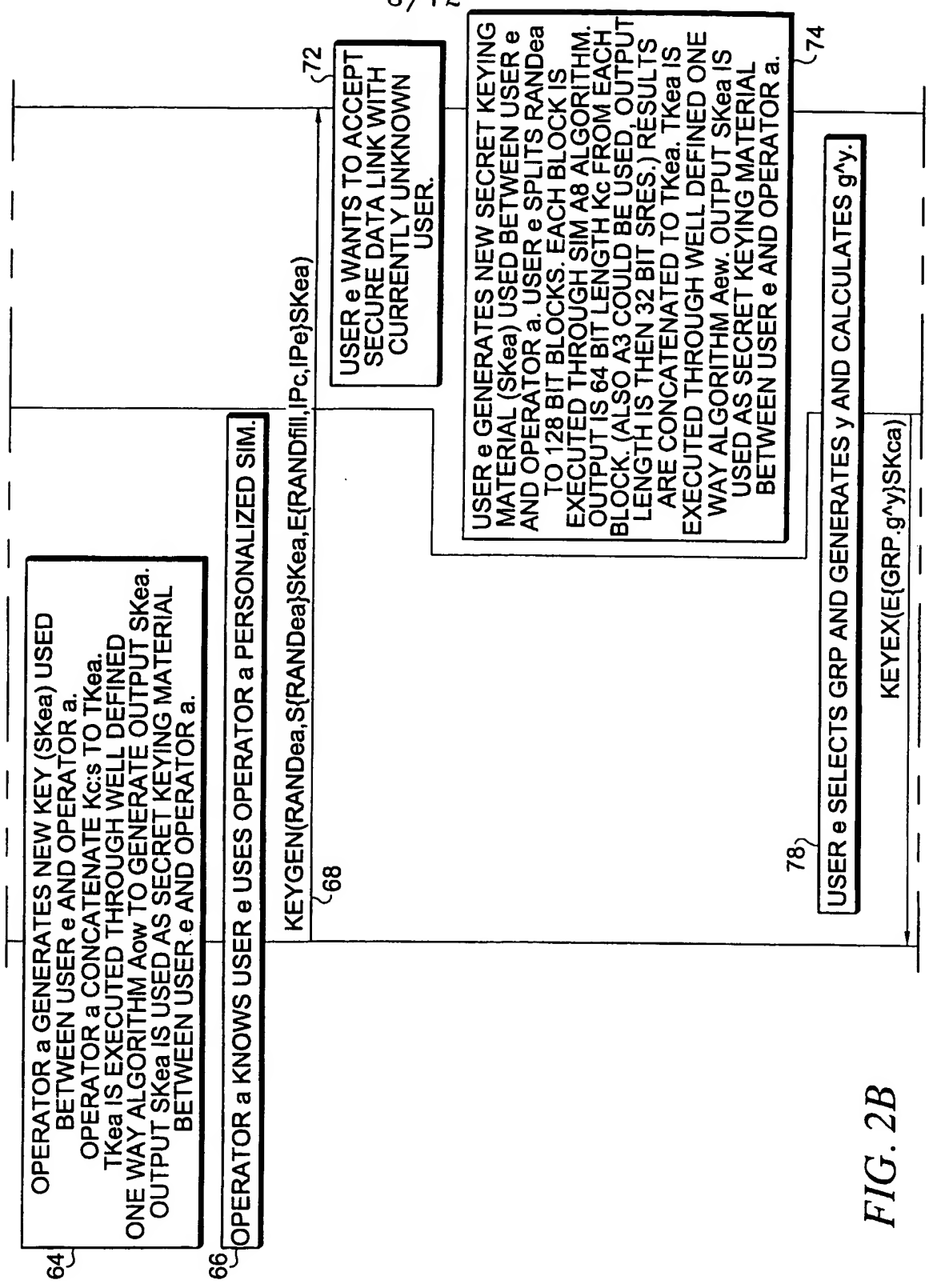

OPERATOR a GENERATES NEW KEY (SKea) USED BETWEEN USER e AND OPERATOR a.
OPERATOR a CONCATENATE Kc:s TO TKea.
TKea IS EXECUTED THROUGH WELL DEFINED ONE WAY ALGORITHM Aow TO GENERATE OUTPUT SKea. OUTPUT SKea IS USED AS SECRET KEYING MATERIAL BETWEEN USER e AND OPERATOR a.
64
OPERATOR a KNOWS USER e USES OPERATOR a PERSONALIZED SIM.
66
KEYGEN(RANDea,S{RANDea}SKea,E{RANDfill,IPc,IPe}SKea)
68
USER e WANTS TO ACCEPT SECURE DATA LINK WITH CURRENTLY UNKNOWN USER.
72
USER e GENERATES NEW SECRET KEYING MATERIAL (SKea) USED BETWEEN USER e AND OPERATOR a. USER e SPLITS RANDea TO 128 BIT BLOCKS. EACH BLOCK IS EXECUTED THROUGH SIM A8 ALGORITHM. OUTPUT IS 64 BIT LENGTH Kc FROM EACH BLOCK. (ALSO A3 COULD BE USED, OUTPUT LENGTH IS THEN 32 BIT SRES.) RESULTS ARE CONCATENATED TO TKea. TKea IS EXECUTED THROUGH WELL DEFINED ONE WAY ALGORITHM Aew. OUTPUT SKea IS USED AS SECRET KEYING MATERIAL BETWEEN USER e AND OPERATOR a.
74
USER e SELECTS GRP AND GENERATES y AND CALCULATES g^y.
78
KEYEX(E{GRP.g^y}SKca)

FIG. 2B

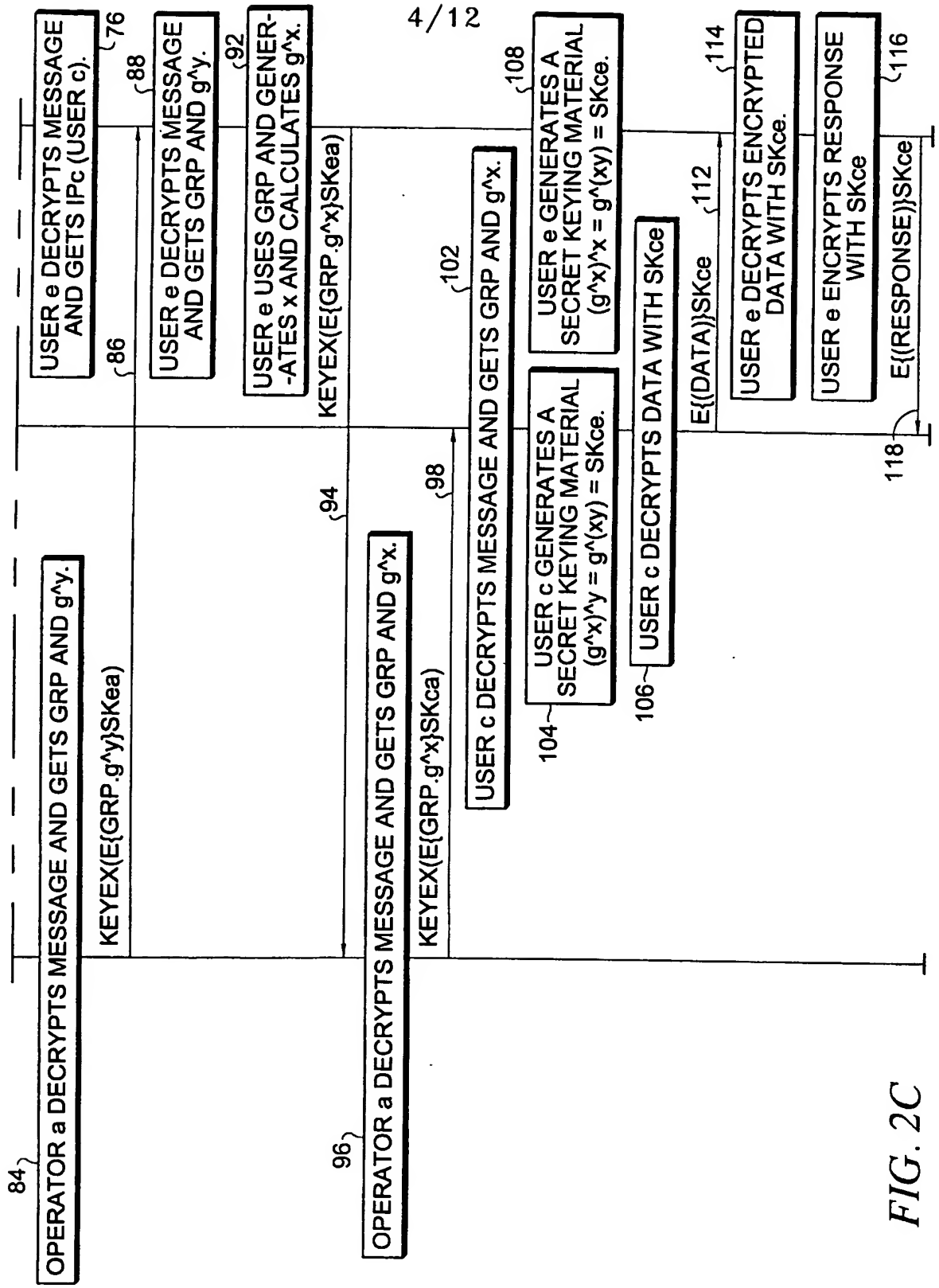

84
OPERATOR a DECRYPTS MESSAGE AND GETS GRP AND g^y.
KEYEX(E{GRP.g^y}SKea)
USER e DECRYPTS MESSAGE AND GETS IPc (USER c).
76
86
USER e DECRYPTS MESSAGE AND GETS GRP AND g^y.
88
USER e USES GRP AND GENER--ATES x AND CALCULATES g^x.
92
KEYEX(E{GRP.g^x}SKea)
94
96
OPERATOR a DECRYPTS MESSAGE AND GETS GRP AND g^x.
KEYEX(E{GRP.g^x}SKca)
98
102
USER c DECRYPTS MESSAGE AND GETS GRP AND g^x.
104
USER c GENERATES A SECRET KEYING MATERIAL (g^x)^y = g^(xy) = SKce.
106
USER c DECRYPTS DATA WITH SKce
108
USER e GENERATES A SECRET KEYING MATERIAL (g^x)^x = g^(xy) = SKce.
112
E{(DATA)}SKce
114
USER e DECRYPTS ENCRYPTED DATA WITH SKce.
USER e ENCRYPTS RESPONSE WITH SKce
116
E{(RESPONSE)}SKce
118

FIG. 2C

FIG. 3A
FIG. 3B
FIG. 3C

FIG. 3

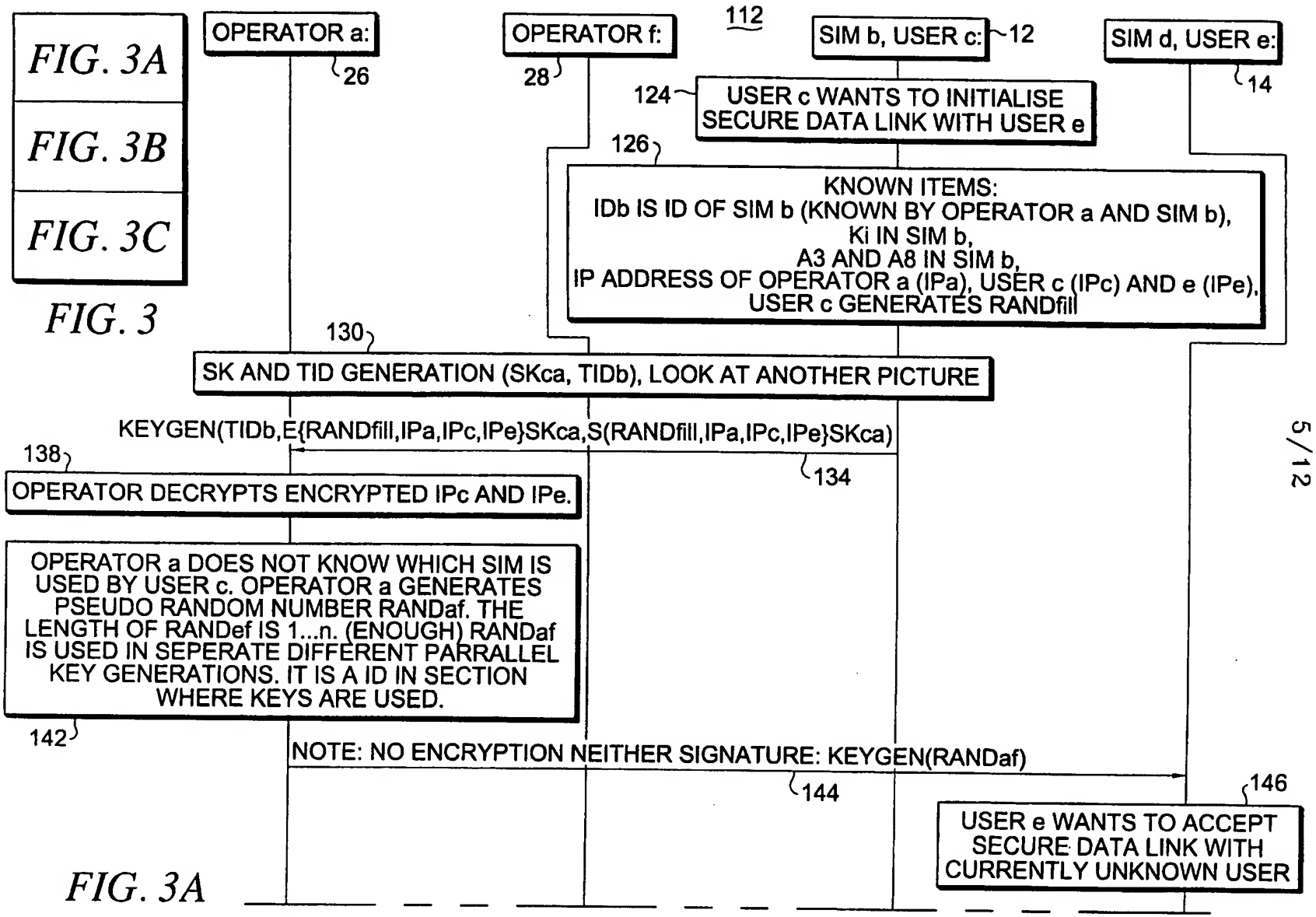


FIG. 3A

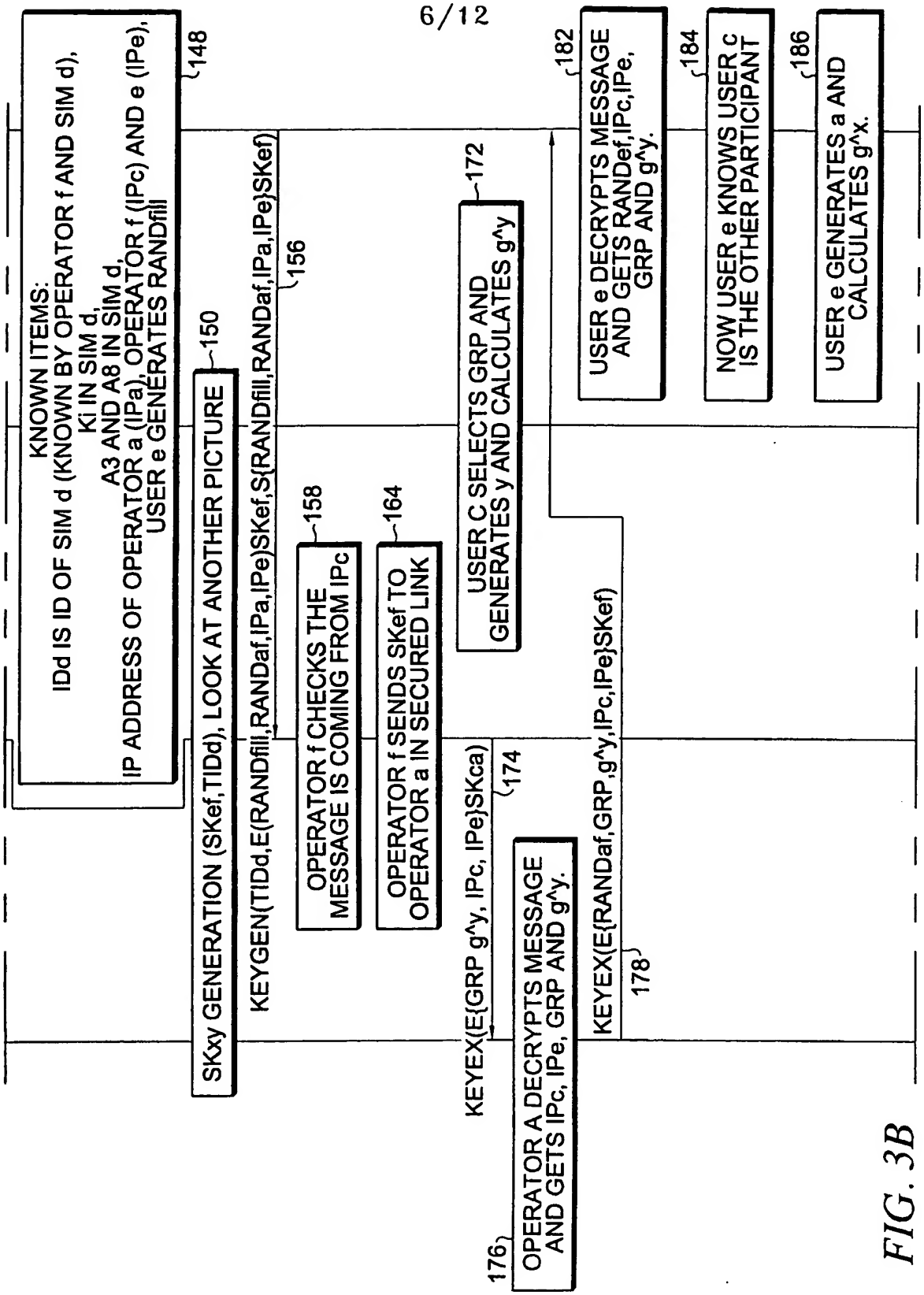

KNOWN ITEMS:
IDd IS ID OF SIM d (KNOWN BY OPERATOR f AND SIM d),
Ki IN SIM d,
A3 AND A8 IN SIM d,
IP ADDRESS OF OPERATOR a (IPa), OPERATOR f (IPc) AND e (IPe),
USER e GENERATES RANDfill
148
SKxy GENERATION (SKef,TIDd), LOOK AT ANOTHER PICTURE
150
KEYGEN(TIDd,E(RANDfill,RANDaf,IPa,IPe)SKef,S(RANDfill,RANDaf,IPa,IPe)SKef)
156
OPERATOR f CHECKS THE MESSAGE IS COMING FROM IPc
158
OPERATOR f SENDS SKef TO OPERATOR a IN SECURED LINK
164
USER C SELECTS GRP AND GENERATES y AND CALCULATES g^y
172
KEYEX(E{GRP g^y, IPc, IPe}SKca)
174
OPERATOR A DECRYPTS MESSAGE AND GETS IPc, IPe, GRP AND g^y.
176
KEYEX(E{RANDaf,GRP,g^y,IPc,IPe}SKef)
178
USER e DECRYPTS MESSAGE AND GETS RANDef,IPc,IPe, GRP AND g^y.
182
NOW USER e KNOWS USER c IS THE OTHER PARTICIPANT
184
USER e GENERATES a AND CALCULATES g^x.
186

FIG. 3B

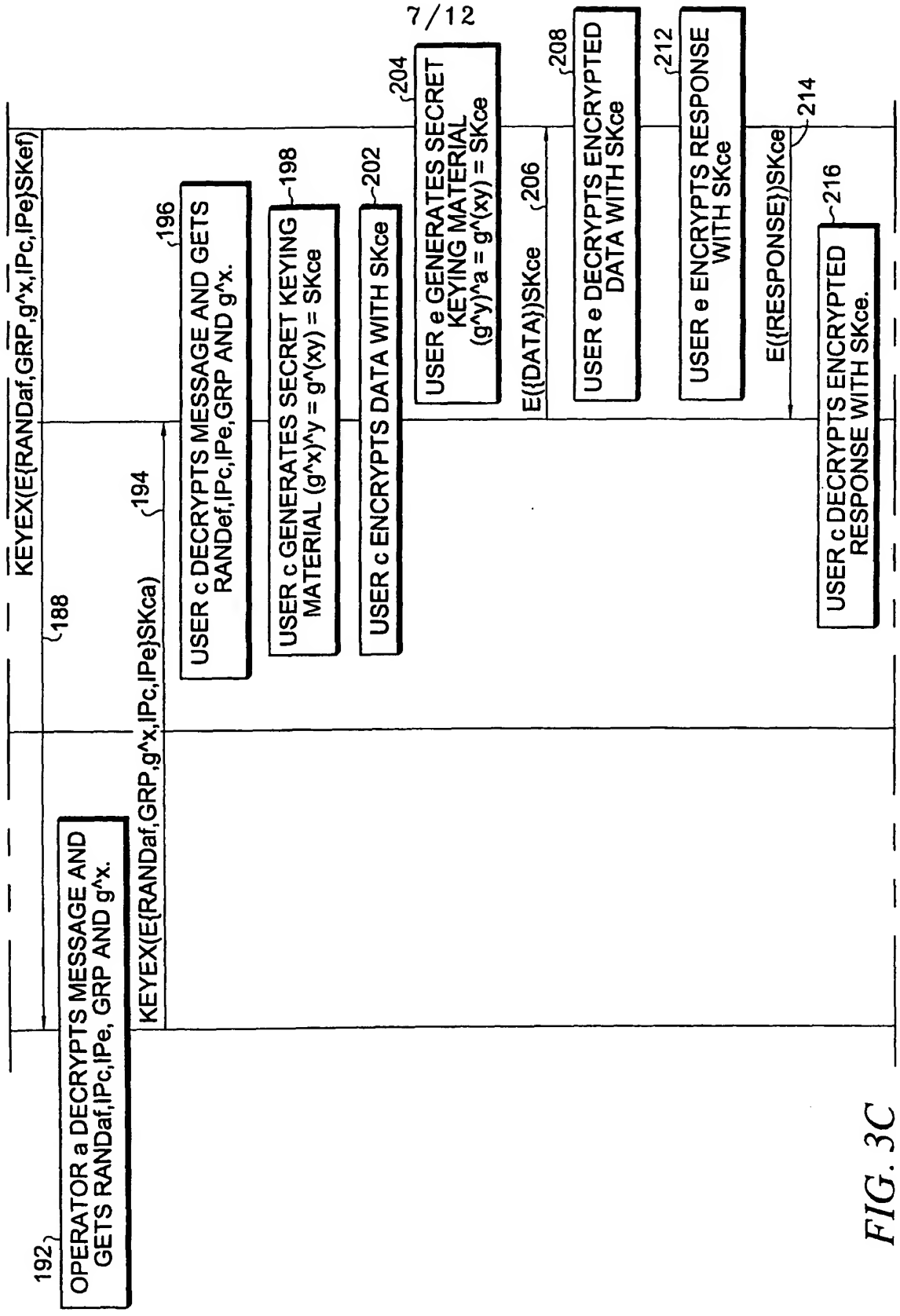

KEYEX(E{RANDaf,GRP,g^x,IPc,IPe}SKef)
188
OPERATOR a DECRYPTS MESSAGE AND GETS RANDaf,IPc,IPe, GRP AND g^x.
192
KEYEX(E{RANDaf,GRP,g^x,IPc,IPe}SKca)
194
USER c DECRYPTS MESSAGE AND GETS RANDef,IPc,IPe,GRP AND g^x.
196
USER c GENERATES SECRET KEYING MATERIAL (g^x)^y = g^(xy) = SKce
198
USER c ENCRYPTS DATA WITH SKce
202
USER e GENERATES SECRET KEYING MATERIAL (g^y)^a = g^(xy) = SKce
204
E{(DATA)}SKce
206
USER e DECRYPTS ENCRYPTED DATA WITH SKce
208
USER e ENCRYPTS RESPONSE WITH SKce
212
E{(RESPONSE)}SKce
214
USER c DECRYPTS ENCRYPTED RESPONSE WITH SKce.
216

FIG. 3C

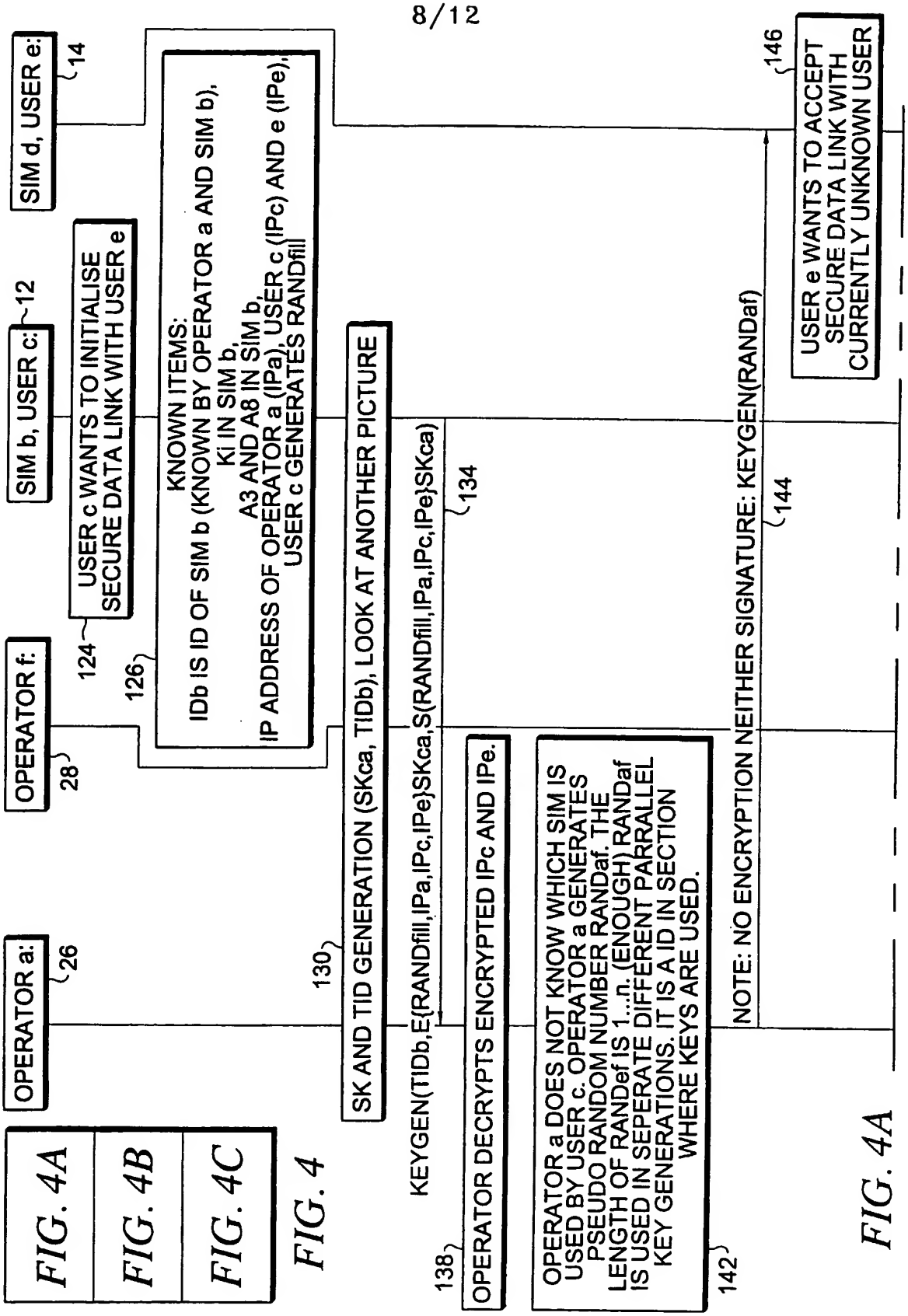


FIG. 4A
FIG. 4B
FIG. 4C

FIG. 4

FIG. 4A

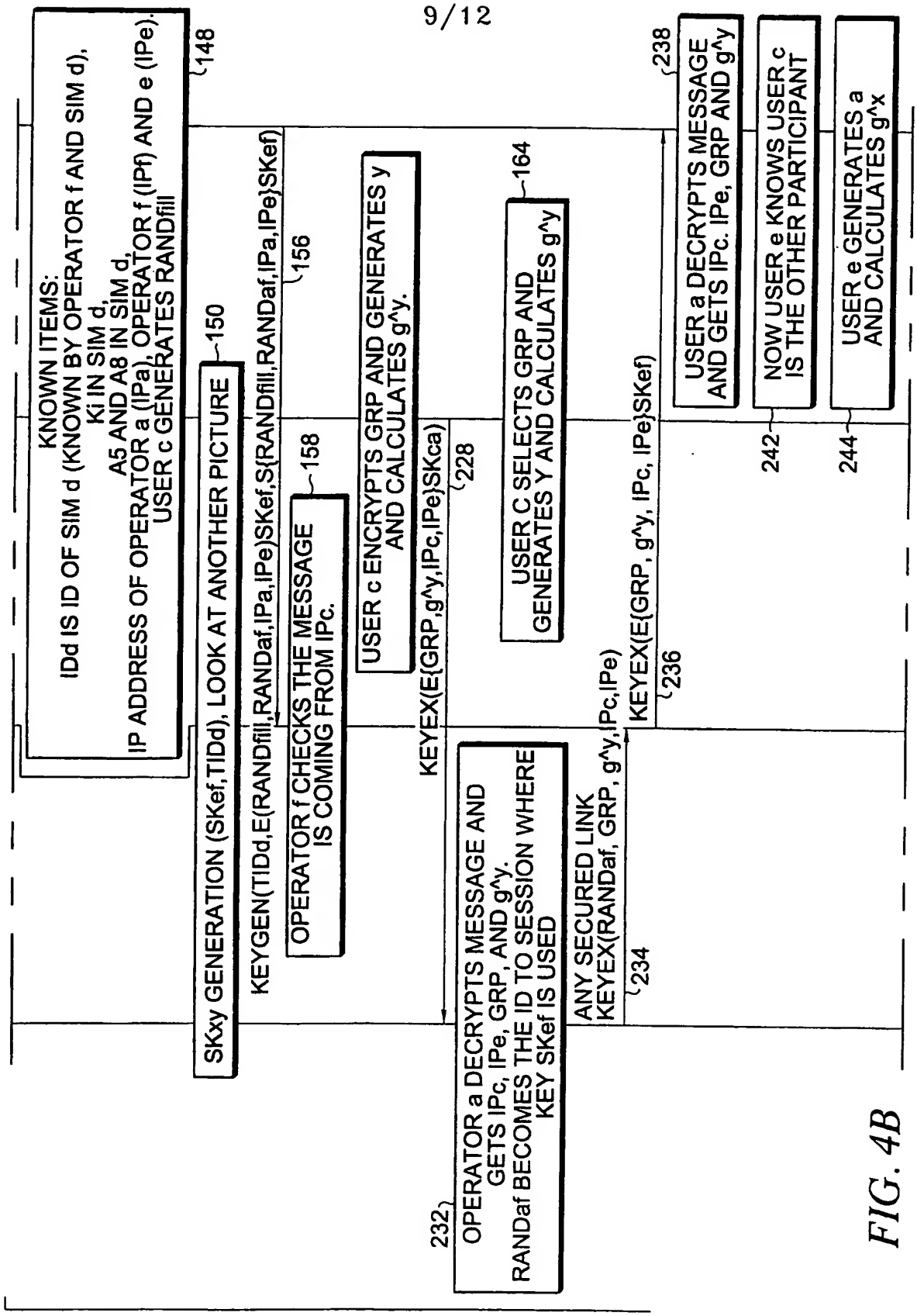

KNOWN ITEMS:
IDd IS ID OF SIM d (KNOWN BY OPERATOR f AND SIM d),
Ki IN SIM d,
A5 AND A8 IN SIM d,
IP ADDRESS OF OPERATOR a (IPa), OPERATOR f (IPf) AND e (IPe).
USER c GENERATES RANDfill
148
SKxy GENERATION (SKef,TIDd), LOOK AT ANOTHER PICTURE
150
KEYGEN(TIDd,E(RANDfill,RANDaf,IPa,IPe)SKef,S(RANDfill,RANDaf,IPa,IPe)SKef)
156
OPERATOR f CHECKS THE MESSAGE IS COMING FROM IPc.
158
USER c ENCRYPTS GRP AND GENERATES y AND CALCULATES g^y.
KEYEX(E{GRP,g^y,IPc,IPe}SKca)
228
USER C SELECTS GRP AND GENERATES Y AND CALCULATES g^y
164
232
OPERATOR a DECRYPTS MESSAGE AND GETS IPc, IPe, GRP, AND g^y.
RANDaf BECOMES THE ID TO SESSION WHERE KEY SKef IS USED
ANY SECURED LINK
KEYEX(RANDaf, GRP, g^y,IPc,IPe)
234
KEYEX(E{GRP, g^y, IPc, IPe}SKef)
236
238
USER a DECRYPTS MESSAGE AND GETS IPc. IPe, GRP AND g^y
242
NOW USER e KNOWS USER c IS THE OTHER PARTICIPANT
244
USER e GENERATES a AND CALCULATES g^x

FIG. 4B

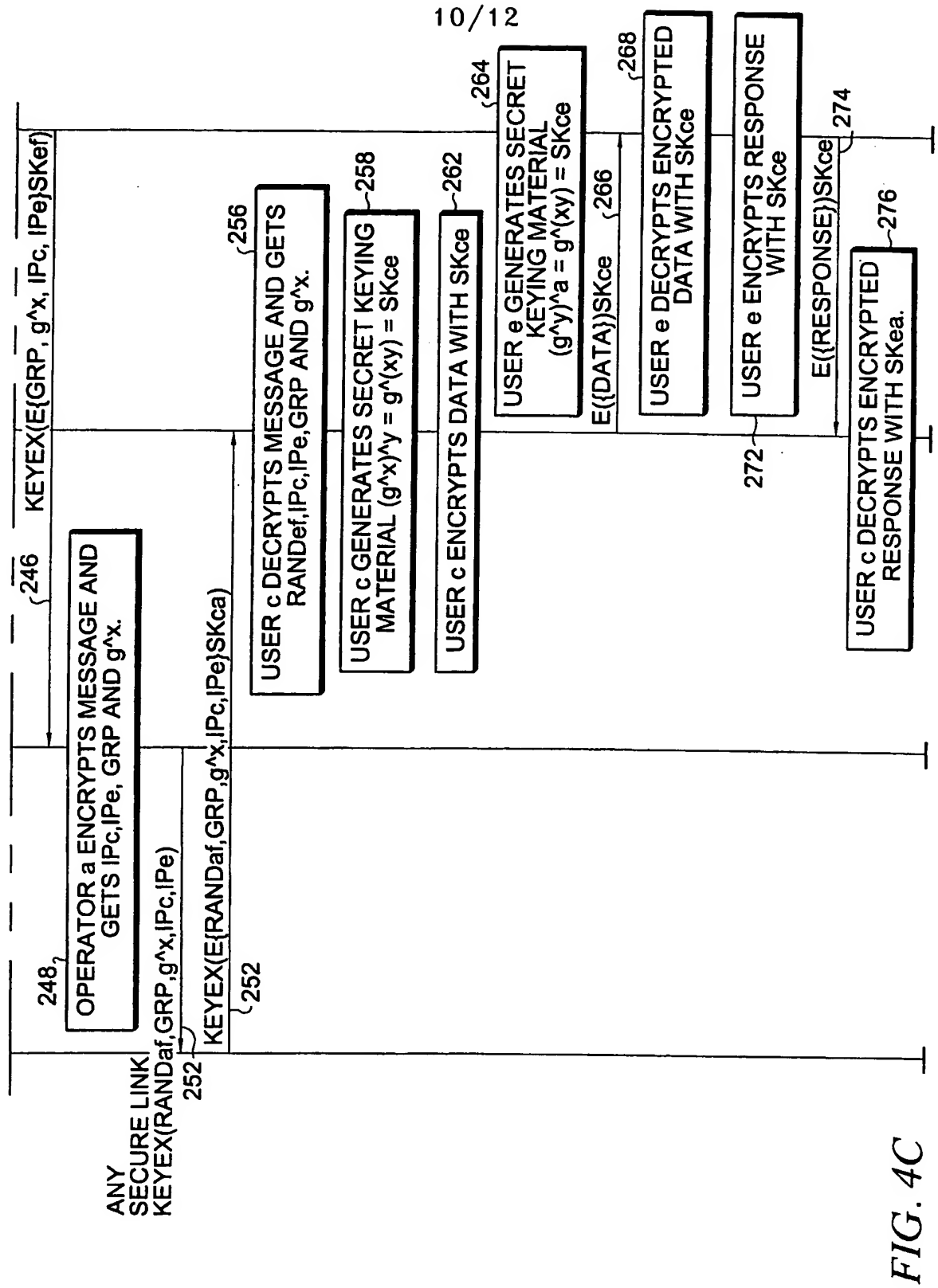

ANY SECURE LINK
KEYEX(RANDaf,GRP,g^x,IPc,IPe)
252
KEYEX(E{RANDaf,GRP,g^x,IPc,IPe}SKca)
252
248
OPERATOR a ENCRYPTS MESSAGE AND GETS IPc,IPe, GRP AND g^x.
246
KEYEX(E{GRP, g^x, IPc, IPe}SKef)
256
USER c DECRYPTS MESSAGE AND GETS RANDef,IPc,IPe,GRP AND g^x.
258
USER c GENERATES SECRET KEYING MATERIAL (g^x)^y = g^(xy) = SKce
262
USER c ENCRYPTS DATA WITH SKce
264
USER e GENERATES SECRET KEYING MATERIAL (g^y)^a = g^(xy) = SKce
266
E({DATA})SKce
268
USER e DECRYPTS ENCRYPTED DATA WITH SKce
272
USER e ENCRYPTS RESPONSE WITH SKce
274
E({RESPONSE})SKce
276
USER c DECRYPTS ENCRYPTED RESPONSE WITH SKea.

FIG. 4C

FIG. 5A
FIG. 5B

FIG. 5

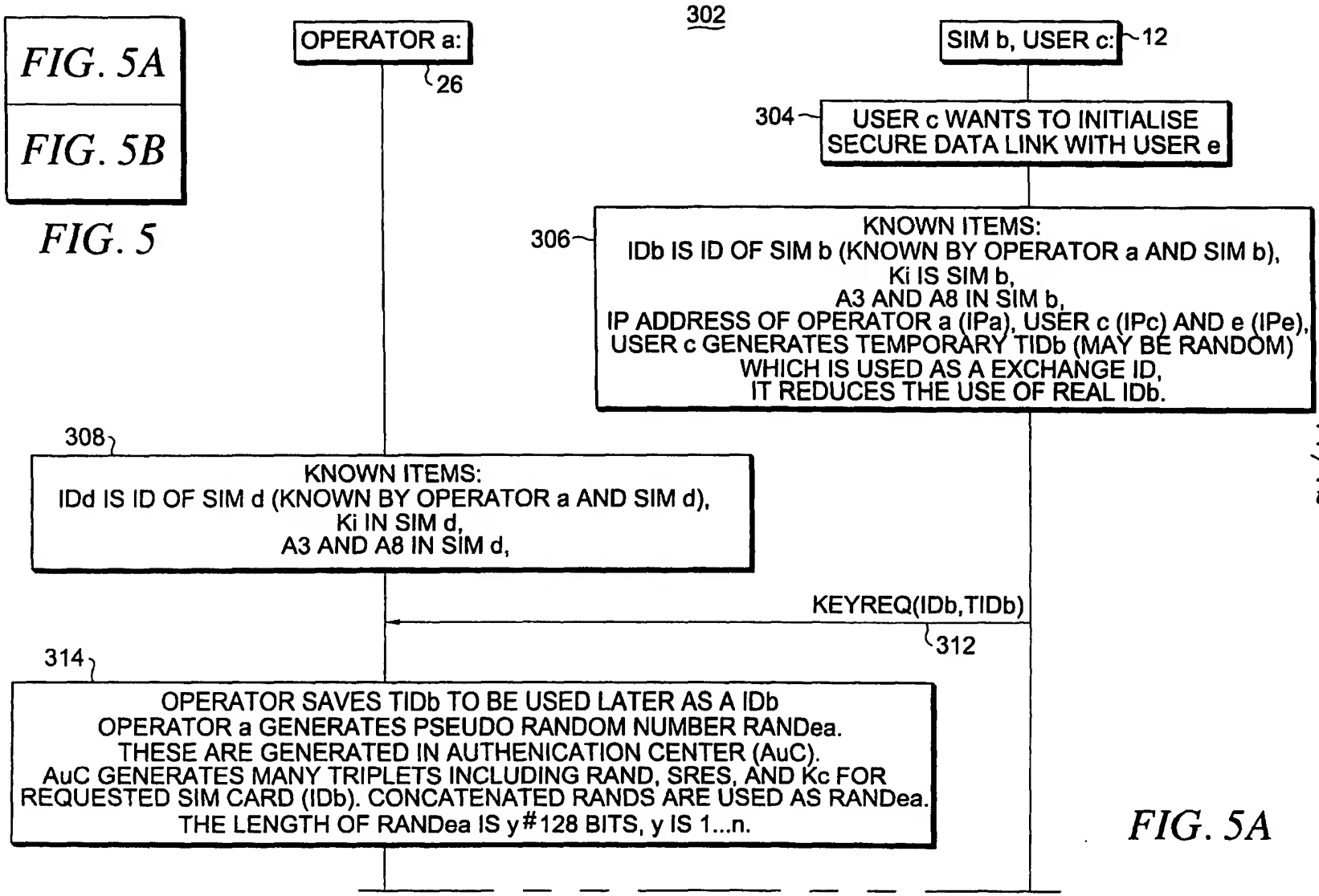


FIG. 5A

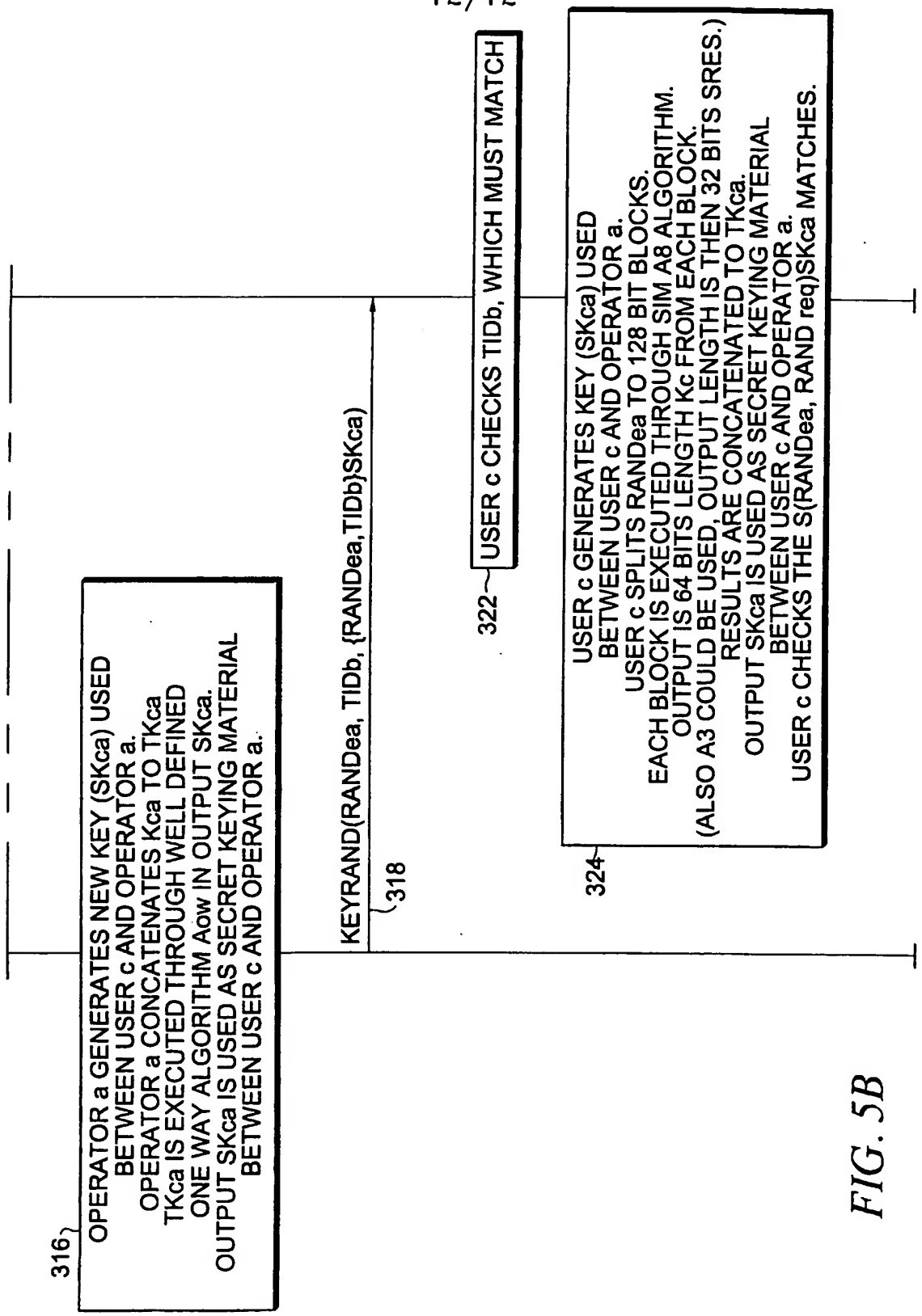

316
OPERATOR a GENERATES NEW KEY (SKca) USED BETWEEN USER c AND OPERATOR a.
OPERATOR a CONCATENATES Kca TO TKca
TKca IS EXECUTED THROUGH WELL DEFINED ONE WAY ALGORITHM Aow IN OUTPUT SKca.
OUTPUT SKca IS USED AS SECRET KEYING MATERIAL BETWEEN USER c AND OPERATOR a.
KEYRAND(RANDea, TIDb, {RANDea,TIDb}SKca)
318
322
USER c CHECKS TIDb, WHICH MUST MATCH
324
USER c GENERATES KEY (SKca) USED BETWEEN USER c AND OPERATOR a.
USER c SPLITS RANDea TO 128 BIT BLOCKS.
EACH BLOCK IS EXECUTED THROUGH SIM A8 ALGORITHM.
OUTPUT IS 64 BITS LENGTH Kc FROM EACH BLOCK.
(ALSO A3 COULD BE USED, OUTPUT LENGTH IS THEN 32 BITS SRES.)
RESULTS ARE CONCATENATED TO TKca.
OUTPUT SKca IS USED AS SECRET KEYING MATERIAL BETWEEN USER c AND OPERATOR a.
USER c CHECKS THE S(RANDea, RAND req)SKca MATCHES.

FIG. 5B